Cryptographie et Sécurité **CT du 19/12/2024**

☐0	☐0	☐0	☐0	☐0	☐0	☐0	☐0	☐0
☐1	☐1	☐1	☐1	☐1	☐1	☐1	☐1	☐1
☐2	☐2	☐2	☐2	☐2	☐2	☐2	☐2	☐2
☐3	☐3	☐3	☐3	☐3	☐3	☐3	☐3	☐3
☐4	☐4	☐4	☐4	☐4	☐4	☐4	☐4	☐4
☐5	☐5	☐5	☐5	☐5	☐5	☐5	☐5	☐5
☐6	☐6	☐6	☐6	☐6	☐6	☐6	☐6	☐6
☐7	☐7	☐7	☐7	☐7	☐7	☐7	☐7	☐7
☐8	☐8	☐8	☐8	☐8	☐8	☐8	☐8	☐8
☐9	☐9	☐9	☐9	☐9	☐9	☐9	☐9	☐9

⟵ codez votre numéro d'étudiant ci-contre en partant de la gauche et écrivez votre nom et prénom ci-dessous. **Si votre numéro d'étudiant contient seulement 6 chiffres, ne noircissez pas la dernière colonne !**

Numéro de copie :

.....

Les questions faisant apparaître le symbole ♣ peuvent présenter zéro, une ou plusieurs bonnes réponses. Les autres ont une unique bonne réponse. Ne noircissez pas les cases dans les zones grisées !!

---

1 El-Gamal

1.1 Enoncés et questions

Alice a rencontré Bob il y a quelques jours. Elle n'a pas eu le temps d'échanger un secret pour discuter de manière sécurisée avec AES CBC. Elle a donc entamé une discussion avec lui par El-Gamal. Le but étant dans un premier temps d'établir un sujet partagé.

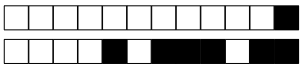
Le générateur qu'elle utilise est $g = 3$. La base qu'elle utilise est $n = 65521$. Elle a choisi un nombre aléatoirement. Sa valeur est 39353. Après avoir effectué la première étape d'El-Gamal, elle a reçu de la part de Bob le message $(47040, 19041)$. Les 6 questions ci-dessous sont liées.

Question 1 D'après la description d'El-Gamal vue en cours, à quoi correspond 47040 ?

- ☐ la demi-clé de Bob
- ☐ la demi-clé d'Alice

Question 2 D'après la description d'El-Gamal vue en cours, à quoi correspond 19041 ?

- ☐ Un chiffrement par multiplication d'un message clair et d'un secret partagé
- ☐ Un chiffrement par xor d'un message clair et d'un secret partagé



Question 3 Posez les calculs à partir des valeurs numériques qui permettront à Alice de découvrir le secret partagé.

☐$-^2$ ☐$-$ ☐n ☐$+$ ☐$+^2$

Répondez sur feuille séparée

Question 4 Posez les calculs à partir des valeurs numériques qui permettront à Alice de découvrir le message chiffré par Bob. Parmi ces calculs devra **obligatoirement** apparaître la trace de la division euclidienne faite par Alice.

☐$-^2$ ☐$-$ ☐n ☐$+$ ☐$+^2$

Répondez sur feuille séparée

Question 5 Parmi les réponses ci-dessous, laquelle correspond au secret partagé ?

- ☐ 42160
- ☐ 56448
- ☐ 60595
- ☐ 10374

Question 6 Parmi les réponses ci-dessous, laquelle correspond au message déchiffré ?

- ☐ 42160
- ☐ 10829
- ☐ 26311
- ☐ 17680

1.2 Aides aux calculs

- Carrés successifs en base 65521 :
  - 47040 51909 58677 58342 38535 43802 29282 27718 53799 7747 64294 64067 17444 13612 58677
  - 19041 31988 56208 47686 48291 62770 33086 24049 534 23072 24580 7259 14197 12213 31573 17835 48291
- Produits en base 65521: 24133 * 19041 = **17680**; 28983 * 19041 = **47441**; 27718 * 34840 = **46622**; 38535 * 60595 = **56448**; 26311 * 58342 = **10374**; 7577 * 64067 = **56091**; 52238 * 19041 = **54978**; 10529 * 19041 = **53950**; 14667 * 19041 = **23845**; 49999 * 19041 = **10829**; 46622 * 53799 = **7577**; 39125 * 19041 = **5355**; 43802 * 56448 = **34840**; 17444 * 56091 = **26311**; 62588 * 19041 = **42160**; 47040 * 58342 = **60595**

2 AES CBC

2.1 Enoncés et questions

Supposons que vous avez trouvé dans l'exercice précédent un secret partagé K : 35612 et un message M : 2121. Attention, les données ici sont très probablement différentes de celles que vous deviez trouver dans l'exercice précédent (pour des raisons évidentes de *reverse-answering*).

Question 7 Parmi les propositions suivantes, laquelle correspond à K : 35612 en hexadécimal ?

- ☐ 763e
- ☐ 8b1c
- ☐ 8cd8
- ☐ 8f19

Question 8 Parmi les propositions suivantes, laquelle correspond au message M : 2121 en hexadécimal ?

- ☐ 1234
- ☐ 5e24
- ☐ 0849
- ☐ b934

A partir de maintenant, nous considérons la clé K sous sa forme hexadécimale comme étant la clé utilisée lors de la session AES CBC d'Alice et Bob. Lors de cette même session, le message M en forme hexadécimale sera considéré comme le vecteur d'initialisation par Alice et Bob.

Question 9

Alice a reçu le message suivant : 0849-68f8-622c. Dessiner le schéma de déchiffrement du mode opératoire CBC que va suivre Alice pour déchiffrer ce message. On prendra soin de reporter sur ce schéma les blocs du message reçu.

☐$^{-2}$ ☐$-$ ☐n ☐$+$ ☐$^{+2}$

Répondez sur feuille séparée

Question 10 Quel message obtenez vous après déchiffrement des blocs 0849-68f8-622c en vous aidant de la table Section 2.2 ?

- ☐ Aie
- ☐ Nope
- ☐ Bref
- ☐ Ouep

2.2 Aides aux calculs

Tables précalculées AES pour le chiffrement :

Hex	Char	Hex	Char	Hex	Char	Hex	Char	Hex	Char	Hex	Char
20	*espace*	30	0	40	@	50	P	60	`	70	p
21	!	31	1	41	A	51	Q	61	a	71	q
22	"	32	2	42	B	52	R	62	b	72	r
23	#	33	3	43	C	53	S	63	c	73	s
24	$	34	4	44	D	54	T	64	d	74	t
25	%	35	5	45	E	55	U	65	e	75	u
26	&	36	6	46	F	56	V	66	f	76	v
27	'	37	7	47	G	57	W	67	g	77	w
28	(	38	8	48	H	58	X	68	h	78	x
29	)	39	9	49	I	59	Y	69	i	79	y
2A	*	3A	:	4A	J	5A	Z	6A	j	7A	z
2B	+	3B	;	4B	K	5B	[	6B	k	7B	{
2C	,	3C	<	4C	L	5C	\	6C	l	7C	|
2D	-	3D	=	4D	M	5D	]	6D	m	7D	}
2E	.	3E	>	4E	N	5E	^	6E	n	7E	~
2F	/	3F	?	4F	O	5F	_	6F	o		

XOR	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
1	1	0	3	2	5	4	7	6	9	8	B	A	D	C	F	E
2	2	3	0	1	6	7	4	5	A	B	8	9	E	F	C	D
3	3	2	1	0	7	6	5	4	B	A	9	8	F	E	D	C
4	4	5	6	7	0	1	2	3	C	D	E	F	8	9	A	B
5	5	4	7	6	1	0	3	2	D	C	F	E	9	8	B	A
6	6	7	4	5	2	3	0	1	E	F	C	D	A	B	8	9
7	7	6	5	4	3	2	1	0	F	E	D	C	B	A	9	8
8	8	9	A	B	C	D	E	F	0	1	2	3	4	5	6	7
9	9	8	B	A	D	C	F	E	1	0	3	2	5	4	7	6
A	A	B	8	9	E	F	C	D	2	3	0	1	6	7	4	5
B	B	A	9	8	F	E	D	C	3	2	1	0	7	6	5	4
C	C	D	E	F	8	9	A	B	4	5	6	7	0	1	2	3
D	D	C	F	E	9	8	B	A	5	4	7	6	1	0	3	2
E	E	F	C	D	A	B	8	9	6	7	4	5	2	3	0	1
F	F	E	D	C	B	A	9	8	7	6	5	4	3	2	1	0

m	0d9e	4a3b
$AES(m)$	622c	68f8

3 Signatures

3.1 Enoncés et questions

Nous avons une fonction de hachage H définie en section 3.2 qui transforme des blocs de 24 bits en blocs de 12 bits. La clé publique RSA de Bob est $(31099, 83)$. Nous ne connaissons pas sa clé privée mais nous la noterons $\texttt{Priv}K_{\text{Bob}}$. Le message >< No tient sur 24 bits. Les deux premiers caractères peuvent

être encodés sur 12 bits comme en TD et tout comme les deux derniers caractères en utilisant la table donnée dans la section 3.2. Bob envoie systématiquement des messages signés. Plus précisément, il envoie des messages composés comme suit :

M, sign($\texttt{PrivK}_{\texttt{Bob}}$,H($M_\#$)) où $M_\#$ est la représentation en entier sur 24 bits de M.

Petit exemple pour illustrer le calcul de $M_\#$ pour M = Baba. $M_\#$: $11 * 16^3 + 36 * 16^2 + 37 * 16^1 + 36 * 16^0 = 50868$

Question 11

Pour le message M : >< No, que vaut $M_\#$?

- ☐ 255715
- ☐ 108078
- ☐ 79128
- ☐ 274338

Question 12

Supposons qu'Alice reçoive M, X où X est la signature prévue construite à partir de M. On suppose que notre configuration RSA est parfaite (même si ce n'est évidemment pas le cas ici avec de petits nombres premiers). On suppose aussi que H n'est pas inversible i.e. à partir d'une donnée y, on ne peut pas deviner une donnée x telle que H(x) = y. Basez vous sur les notations $M_\#$, (31099, 83), X et H pour expliquer comment Alice peut vérifier que le message (message + signature) a bien été construit par Bob.

☐$-^2$ ☐$-$ ☐n ☐$+$ ☐$+^2$

Répondez sur feuille séparée

Question 13 Parmi les réponses ci-dessous, laquelle correspond à la signature par Bob du message ><No sachant que ce dernier a respecté le procédé décrit au début de la section 3 ?

- ☐ 17491
- ☐ 4312
- ☐ 12583
- ☐ 10357

3.2 Aides aux calculs

Carrés successifs et produits en base 31099

- 12583, 6880, 1722, 10879, 20946, 21323, 2949, 19980, 13636
- 17491, 14218, 8024, 9646, 28207, 29132, 12813, 1348, 13362
- 4312, 27241, 18842, 25879, 5676, 29511, 2725, 24063, 26787
- 10357, 6998, 22178, 1900, 2516, 17159, 17048, 14149, 9938
- 12813 * 23864 = **4064**; 14218 * 17491 = **19434**; 19434 * 28207 = **23864**; 20946 * 22523 = **26027**; 2949 * 26027 = **1291**; 6880 * 12583 = **22523**; 2269 * 5676 = **3858**; 2725 * 3858 = **1588**; 4312 * 27241 = **2269**; 2516 * 17616 = **5781**; 5781 * 17048 = **1757**; 6998 * 10357 = **17616**

	0	1	2	3	4	5	6	7	8	9
0	0	1	2	3	4	5	6	7	8	9
1	A	B	C	D	E	F	G	H	I	J
2	K	L	M	N	O	P	Q	R	S	T
3	U	V	W	X	Y	Z	a	b	c	d
4	e	f	g	h	i	j	k	l	m	n
5	o	p	q	r	s	t	u	v	w	x
6	y	z	<	>						

Tableau pour la fonction H :

m	274338	79128	108078	255715	81907	83231	79399	79566
H(m)	4064	1291	1588	1757	4064	1291	1588	1757

4 Maîtrise RSA

4.1 Enoncés et questions

Alice et Bob ont chacun établi une paire de clé RSA : $(n, e_A)/(n, d_A)$ pour Alice et $(n, e_B)/(n, d_B)$ pour Bob. Ici $n = 44920657$, $e_A = 133$ et $e_B = 233$ sont les seules valeurs connues. Nous savons qu'Alice a envoyé un message M chiffré avec la clé publique de Bob $((n, e_B))$ et que Bob a également chiffré exactement le même message avec la clé publique d'Alice (n, e_A). Ces deux messages chiffrés sont respectivement : 29638352 et 20628685.

Question 14
Décrivez comment, en ne connaissant aucune des clés privées, on peut retrouver, ce cas précis, le message M clair (sous sa forme d'entier). Prenez vous pour Euclide et détaillez mathématiquement toute votre méthode en l'illustrant par vos calculs.

☐$-^2$ ☐$-$ ☐n ☐$+$ ☐$+^2$

Répondez sur feuille séparée

Question 15 **Attention : répondre à cette question peut vous retirer des points en cas d'erreur** Sachant que l'entier trouvé à la question précédente est initialement un nombre prévu sur 24 bits, retrouvez le message de 4 caractères encodé comme expliqué dans la section 3.1.

- ☐ Huum
- ☐ Noon
- ☐ $< 3 < 3$
- ☐ Cool

4.2 Aides aux calculs

- **Théorème des restes chinois** : $\forall \alpha \in \mathbb{N}, \beta \in \mathbb{N}$ (pour tout), si $\mathrm{pgcd}(\alpha, \beta) = 1$, alors il existe des coefficients $a \in \mathbb{N}$ et $b \in \mathbb{N}$ tels que $a * \alpha + b * \beta = 1$.
- $\forall x, k, k' \in \mathbb{N}$, $(x^k)^{k'} = x^{k*k'}$.
- $\forall x, k, k' \in \mathbb{N}$, $(x^k) * x^{k'} = x^{k+k'}$.
- $\mathrm{PGCD}(133, 233) = 1$
- Quelques carrés successifs en base 44920657
  - 20628685, 7412883, 23552787, 2328882, 16164401, 30308437, 16634686
  - 29638352, 16557388, 11205418, 25600807, 39131163, 18745631, 14265797
  - 23050148, 10244608, 43868719, 43011963, 2582279, 7746790, 15330496
- Quelques produits intéressants : 11305605 * 6306056 = **23836552**; 408259 * 428098 = **33505652**; 12550547 * 364419 = **16174081**; 15236720 * 23552787 = **62799**; 7812174 * 14687236 = **26179616**; 1604498 * 2175757 = **33816888**; 2731515 * 596973 = **20854995**
- Pour calculer x^{-y} avec x et y deux entiers positifs, cela revient à faire $(x^{-1})^y$